**COMPUTER NETWORKS – PACKAGE**

**ABSTRACT**

**PACKAGE TITLE**

Firewall Configuration and Testing

**TEAM MEMEBERS**

VARUN G - 23PC38

AKSHAY SK - 23PC05

**MODULES AND TOOLS USED**

scanpy, os, sys, socket - Modules in Python

iptables/iptables-legacy – Defining firewall rules

Kali Linux – Working Environment

**ABSTRACT ABOUT THE PROJECT**

This project presents a Simple Python Firewall and Penetration Testing Tool, designed to configure and test basic firewall rules using Python and iptables on Linux systems. The firewall allows users to define default policies, permit specific IP addresses and services, and block designated ports. It uses the python-iptables (iptc) module to programmatically enforce these rules, while maintaining logs for transparency and auditing. It scans a range of ports, verifies access to allowed services, ensures blocked ports are inaccessible, and confirms the default policy behaviour validating the firewall’s configuration. Additionally, it simulates basic denial-of-service attack, an ICMP flood attack, to evaluate the firewall's resilience under network stress. These simulations help assess the firewall’s capability to handle real-world attack vectors.